



DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DoD-2022-OS-0061]

Privacy Act of 1974; System of Records

AGENCY: Office of Inspector General, Department of Defense (DoD).

ACTION: Notice of a modified system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the DoD is modifying and reissuing a current system of records titled, “Defense Case Activity Tracking System (D-CATS),” CIG-16. The system of records is being retitled, “Inspector General Administrative Investigation Records (IGAIR).” This system of records was originally established by the DoD Office of Inspector General (OIG) to collect and maintain records on individuals who file DoD Hotline complaints and individuals suspected of misconduct and investigated pursuant to the Inspector General Act of 1978, as amended. This system of records notice (SORN) is being updated to incorporate the DoD standard routine uses and support additional information sharing of records outside of the DoD in furtherance of external oversight, case management, and required reporting. This modification revises the system name, system location, system manager, authority for maintenance, purpose, categories of individuals, categories of records, record source categories, routine uses, policies, and practices for retention and disposal of records, policies and practices for retrieval of information, information safeguards, record access procedures, contesting records, and notification procedures and the exemptions promulgated. Additionally, the DoD will issue a Notice of Proposed Rulemaking proposing to exempt this system of records from certain provisions of the Privacy Act in a future issue of the *Federal Register*.

DATES: This system of records is effective upon publication; however, we will accept comments on the Routine Uses on or before **[INSERT DATE 30 DAYS AFTER DATE OF**

PUBLICATION IN THE FEDERAL REGISTER]. The Routine Uses are effective at the close of the comment period.

ADDRESSES: You may submit comments, identified by docket number and title, by any of the following methods:

* Federal Rulemaking Portal: <https://www.regulations.gov>. Follow the instructions for submitting comments.

* Mail: Department of Defense, Office of the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency, Regulatory Directorate, 4800 Mark Center Drive, Attn: Mailbox 24, Suite 08D09, Alexandria, VA 22350-1700.

Instructions: All submissions received must include the agency name and docket number for this *Federal Register* document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the Internet at <https://www.regulations.gov> as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: Anna Rivera, Government Information Specialist, DoD OIG FOIA, Privacy and Civil Liberties Office, Department of Defense, Office of Inspector General, 4800 Mark Center Drive, Alexandria, VA 22350-1500, privacy@dodig.mil, or phone number (703) 699-5680.

SUPPLEMENTARY INFORMATION:

I. Background

The DoD OIG maintains this system of records in order to carry out its responsibilities pursuant to the Inspector General Act of 1978, as amended. The DoD OIG is statutorily authorized to conduct as well as engage in oversight of investigations relating to the programs and operations of the DoD; to promote economy, efficiency, and effectiveness in the administration of such programs and operations; and to prevent and detect fraud, waste, and abuse in such programs and operations. Specifically, the CIG-16 IG AIR system of records

(hereafter, IG AIR) contains records of DoD OIG mission activities such as the identification, referral, and investigation of DoD Hotline complaints. The DoD Hotline provides a confidential avenue for individuals to report allegations of wrongdoing pertaining to programs, personnel, and operations that fall under the purview of the DoD, pursuant to the Inspector General Act.

IG AIR also contains records of administrative investigations of both military and civilian senior officials accused of misconduct. In addition, it contains records related to the oversight and investigation of whistleblower reprisal cases against Service members, DoD contractor employees, and DoD civilian employees (appropriated and non-appropriated fund). These records also include the improper command referrals of Service member mental health evaluations. IG AIR is critical to the DoD OIG's management and oversight of DoD programs and activities and is used for case management, information storage, to respond to requests for information, and to fulfill mandatory reporting requirements.

Subject to public comment, the DoD is updating the Routine Uses section of this SORN by removing the incorporation by reference of the DoD blanket routine uses, adding the standard DoD routine uses (A through J), revising routine uses (K through M), and adding new routine uses (N through Z) allowing for additional disclosures outside the DoD. In addition to modifications made to the routine uses section, other modifications are as follows: (1) revise the system name in the System Name and Number section; (2) update office and address in the System Location section; (3) add updated information in the System Manager section; (4) add citations in the Authority for Maintenance of the System section; (5) add information regarding the purpose of the system in the Purpose section; (6) broaden types of information in the Categories of Individuals, Categories of Records, and Record Source Categories sections; (7) provide records retrieval, retention, and disposition guidance in the Policies and Practices for Retrieval of Records and the Policies and Practices for Retention and Disposal of Records sections; (8) update the security requirements in the Administrative, Technical, and Physical Safeguards section; (9) update guidance, citation, and information needed to submit request in

the Record Access Procedures, Contesting Record Procedures, and Notification Procedures sections and (10) update to the Exemptions Promulgated for the System section to claim exemptions from certain provisions of the Privacy Act for classified information in this system of records. Furthermore, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice.

The DoD will issue a Notice of Proposed Rulemaking proposing to exempt this system of records from certain provisions of the Privacy Act in a future issue of the *Federal Register*. This rulemaking will seek public comment on the recently added exemption under 5 U.S.C. 552a(k)(1) as well as a previously claimed exemption under 5 U.S.C. 552a(j)(2) for which a rulemaking was not completed.

DoD SORNs have been published in the *Federal Register* and are available from the address in FOR FURTHER INFORMATION CONTACT or at the Defense Privacy, Civil Liberties, and Freedom of Information Directorate website at <https://dpclld.defense.gov>.

II. Privacy Act

Under the Privacy Act, a “system of records” is a group of records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined as a U.S. citizen or lawful permanent resident.

In accordance with 5 U.S.C. 552a(r) and Office of Management and Budget (OMB) Circular No. A-108, DoD has provided a report of this system of records to the OMB and to Congress.

Dated: May 24, 2022.

Aaron T. Siegel,

Alternate OSD Federal Register Liaison Officer,

Department of Defense.

SYSTEM NAME AND NUMBER: Inspector General Administrative Investigation Records (IGAIR), CIG-16.

SECURITY CLASSIFICATION: Unclassified; Classified.

SYSTEM LOCATION: Department of Defense (Department or DoD), located at 1000 Defense Pentagon, Washington, DC 20301-1000, and other Department installations, offices, or mission locations. Information may also be stored within a government-certified cloud, implemented and overseen by the Department's Chief Information Officer, 6000 Defense Pentagon, Washington, DC 20301-6000.

SYSTEM MANAGER(S): Deputy Inspector General for Administrative Investigations, Office of Inspector General (OIG), DoD, 4800 Mark Center Drive, Alexandria, VA 22350-1500, 703-604-8799.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Inspector General Act of 1978, as amended; 10 U.S.C. 113, Secretary of Defense; 10 U.S.C. 141, Inspector General; DoD Directive (DoDD) 5106.01, Inspector General of the Department of Defense; and DoDD 5106.04, Defense Inspectors General.

PURPOSE(S) OF THE SYSTEM: This system supports the DoD OIG, its staff and investigators in the receipt and evaluation of complaints, conduct and supervision of investigations and associated activities within the DoD OIG's jurisdiction, specifically:

A. To receive, document, evaluate, track, oversee, manage, resolve, and respond to complaints and allegations made by an individual and received by the DoD OIG through the DoD Hotline. This includes reports of allegations of wrongdoing pertaining to programs, personnel, and operations that fall under the purview of the DoD, pursuant to the Inspector General Act, as well as other complaints or allegations received which may be outside of the DoD OIG's jurisdiction.

B. To support the conduct of OIG-led administrative investigations and oversee DoD Component-led administrative investigations pertaining to programs, personnel, and operations

that fall under the purview of the DoD, to include misconduct allegations against military and civilian senior officials, investigations into alleged whistleblower reprisal against Service members, DoD contract employees, and DoD civilian employees; alleged Service member restriction from communication with an IG or Member of Congress; and improper command referrals of Service members for mental health evaluations. This system also supports the storage of records and information documenting evidence, statements, reports, and notifications associated with these investigative activities.

Note 1: DoD OIG criminal investigation records are excluded from this system of records and instead covered by the CIG-04 Case Reporting and Information Management System of Records, and CIG-06 Investigative Files System of Records Notices (SORNs). DoD OIG may also refer allegations of criminal misconduct to the Defense Criminal Investigative Service or other criminal investigative units of DoD components, in which case the criminal investigative records would be covered by the DoD-0006 Military Justice and Civilian Criminal Case Records SORN or other applicable SORNs published by those components.

Note 2: Complaint and investigation records appearing to involve Equal Employment Opportunity (EEO) issues are excluded from this system of records. Those records are covered by the EEOC/GOVT-1 Equal Employment Opportunity in the Federal Government Complaint and Appeals Records SORN.

Note 3: Investigative records of alleged misconduct by DoD OIG personnel are excluded from this system of records. Those records are covered by the CIG-26 Case Control System – Investigative SORN.

C. To support mandatory reporting requirements, the compilation of statistical information, the provision of data for analysis and decision-making, and the response to requests for information, related to the activities described above.

D. To identify and address conduct that may warrant criminal or disciplinary action, to uphold and enforce the law, and to ensure public safety.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

A. For complaints and allegations made by an individual and received by the DoD OIG through the DoD Hotline: any individual who reports allegations of wrongdoing pertaining to programs, personnel, and operations (complainant).

B. For OIG-led administrative investigations and DoD Component-led administrative investigations pertaining to programs, personnel, and operations that fall under the purview of the DoD: any individual who is the subject of an investigation into alleged administrative misconduct within DoD's investigatory jurisdiction, including but not limited to, violations of laws, rules, or regulations; fraud, waste, and abuse; mismanagement or abuse of authority; and whistleblower reprisal. These records may also include information about other types of individuals who are not covered by the system for purposes of these records, such as complainants, witnesses, and DoD OIG and DoD component staff and investigators.

CATEGORIES OF RECORDS IN THE SYSTEM: Categories of records may include:

A. Personal Information, such as: full name and aliases; DoD ID number; date of birth; home address and e-mail address; phone numbers; place of birth; citizenship/immigration status; race/ethnicity; medical information/medical records; biometric data; driver's license number; vehicle registration information; marital status; gender/gender identification; and biographical data.

B. Employment Information, such as: duty position/title, rank/grade, and duty station; work address and e-mail address; supervisor's name and contact information; military records; personnel records; financial information; and education and training records.

C. Complaint / Allegation Information, such as: the specific allegations or complaints of misconduct, including any supporting documentation or other materials, received by the DoD OIG from individuals, and the date/time of receipt by DoD OIG.

D. Investigative Information, such as: case numbers; investigative data (including investigative findings and reports); supporting exhibits and data in any form (including papers,

photographs, electronic recordings, electronic data, or videos lawfully acquired from any source); forms; disposition data associated with adverse actions or administrative actions; complainant, subject, and witness statements; notifications; criminal history; information received from other governmental agencies and other sources pertaining to an investigation; and case referrals from other agencies.

RECORD SOURCE CATEGORIES: Records and information stored in this system of records are obtained from: Individuals (such as complainants, subjects, and witnesses); foreign, international, Federal, State, and local government agencies or entities; private businesses; nonprofit organizations; Internet websites; and other publicly available information.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING

CATEGORIES OF USERS AND PURPOSES OF SUCH USES: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, all or a portion of the records or information contained herein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal government when necessary to accomplish an agency function related to this system of records.

B. To the appropriate Federal, State, local, territorial, tribal, foreign, or international law enforcement authority or other appropriate entity where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether criminal, civil, or regulatory in nature.

C. To any component of the Department of Justice (DOJ) for the purpose of representing the DoD, or its components, officers, employees, or members in pending or potential litigation to which the record is pertinent.

D. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body or official, when the DoD or other Agency representing the DoD determines that the

records are relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

E. To the National Archives and Records Administration for the purpose of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

F. To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

G. To appropriate agencies, entities, and persons when (1) the DoD suspects or confirms a breach of the system of records; (2) the DoD determines as a result of the suspected or confirmed breach there is a risk of harm to individuals, the DoD (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the DoD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

H. To another Federal agency or Federal entity, when the DoD determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

I. To another Federal, State or local agency for the purpose of comparing to the agency's system of records or to non-Federal records, in coordination with an Office of Inspector General in conducting an audit, investigation, inspection, evaluation, or other review as authorized by the Inspector General Act of 1978, as amended.

J. To such recipients and under such circumstances and procedures as mandated by Federal statute or treaty.

K. To designated officers, contractors, and employees of Federal, State, local, territorial, tribal, international, or foreign agencies for the purpose of the hiring or retention of an individual, the conduct of a suitability or security investigation, the letting of a contract, or the issuance of a license, grant or other benefit, to the extent that the information is relevant and necessary to the agency's decision on the matter and that the employer is appropriately informed about information that relates to or may impact an individual's suitability or eligibility.

L. To the news media and the public, with the approval of the DoD Inspector General in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information, when disclosure is necessary to preserve confidence in the integrity of DoD, or when disclosure is necessary to demonstrate the accountability of DoD's officers, employees, or individuals covered by the system, except to the extent the Inspector General determines that release of the specific information in the context of a particular case would constitute a clearly unwarranted invasion of personal privacy.

M. To complainants and/or subjects to the extent necessary to provide such persons with information and explanations concerning the progress and/or results of an investigation or case arising from the matters of which they complained and/or which they were a subject.

N. To other Federal Inspector General offices, the Council of the Inspectors General on Integrity and Efficiency (CIGIE), or other law enforcement agencies for the purpose of coordinating and conducting audits, reviews, administrative inquiries, civil or criminal investigations, or when responding to such offices in connection with the investigation of potential violation of law, rule, and/or regulation.

O. To other Federal IG offices, CIGIE, and/or the DOJ for purposes of conducting external reviews to ensure that adequate internal safeguards and management procedures continue to exist within the DoD.

P. To the DOJ and other Federal, State, or local government prosecuting or litigating agencies, for the purpose of satisfying obligations under *Giglio* (405 U.S. 150 (1972)) and *Henthorn* (931 F.2d 29 (9th Cir. 1991)), as well as the DOJ United States Attorneys' Manual, Section 9-5.100 and DoD IG Instruction 5500.1, DOJ Requirements for Potential Impeachment Information (Giglio Policy), or DoD OIG initiated notifications of similar information.

Q. To the Office of Management and Budget (OMB), for the purpose of private relief legislation review as set forth in OMB Circular A-19 at any stage of the legislative coordination and clearance process as set forth in that circular.

R. To the appropriate Federal, State, local, territorial, tribal, foreign, or international law enforcement authority or other appropriate entity, where a record, either alone or in conjunction with other information, indicates a violation or potential violation of administrative standards or indicates a threat or potential threat to individual or public health or safety.

S. To a former DoD employee for the purpose of responding to an official inquiry by a Federal, State, local, territorial or tribal entity or professional licensing authority, in accordance with applicable DoD regulations; or for the purpose of facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the DoD requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

T. To the Merit Systems Protection Board and the Office of the Special Counsel for the purpose of litigation, including administrative proceedings, appeals, special studies of the civil service, and other merit systems; review of the Office of Personnel Management (OPM) or component rules and regulations; investigation of alleged or possible prohibited personnel practices, including administrative proceedings involving any individual subject of a DoD investigation.

U. To OPM for the purpose of addressing civilian pay and leave, benefits, retirement deduction, and any other information necessary for OPM to carry out its legally authorized government-wide personnel management functions and studies.

V. To State and local taxing authorities with which the Secretary of the Treasury has entered into agreements under 5 U.S.C. 5516, 5517, or 5520 and only to those State and local taxing authorities for which an employee or Service member is or was subject to tax regardless of whether tax is or was withheld. The information disclosed is information normally contained in Internal Revenue Service (IRS) Form W-2.

W. To Federal, State, local, territorial, tribal, international, or foreign criminal, civil, or regulatory law enforcement authorities when the information is necessary for collaboration, coordination, and de-confliction of investigative matters, prosecutions, and/or other law enforcement actions to avoid duplicative or disruptive efforts and to ensure the safety of law enforcement officers who may be working on related law enforcement matters.

X. To the Department of State when it requires information to consider and/or provide an informed response to a request for information from a foreign, international, or intergovernmental agency, authority, or organization about enforcement matter with transnational implications.

Y. To Federal, State, local, tribal, territorial, or foreign government agencies, as well as to other individuals and organizations during the course of an investigation by DoD or the processing of a matter under DoD's jurisdiction, when DoD deems that such disclosure is necessary to carry out its functions and statutory mandates or to elicit information required by DoD to carry out its functions and statutory mandates.

Z. To federal and foreign government intelligence or counterterrorism agencies or components when DoD becomes aware of an indication of a threat or potential threat to national or international security, or when such disclosure is to support the conduct of national intelligence and security investigations or to assist in anti-terrorism efforts.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records may be stored electronically or on paper in secure facilities in a locked drawer and/or behind a locked door. The records may be stored on magnetic disc, tape, or digital media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records are retrieved as follows:

For complaints and allegations made by an individual and received by the DoD OIG through the DoD Hotline: by the name of the complainant or the number assigned to the complaint or allegation.

For OIG-led administrative investigations and DoD Component-led administrative investigations pertaining to programs, personnel, and operations that fall under the purview of the DoD: by the name of the subject or the investigative case number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are retained and disposed of in accordance with applicable disposition schedules. Any unscheduled records are retained indefinitely until they have been scheduled with National Archives and Records Administration and have become eligible for disposition under those schedules.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: The DoD OIG safeguards records in this system of records according to applicable rules, policies, and procedures, including all applicable DoD automated systems security and access policies. DoD policies require the use of controls to minimize the risk of compromise of personally identifiable information (PII) in paper and electronic form and to enforce access by those with a need to know and with appropriate clearances. Additionally, DoD has established security audit and accountability policies and procedures which support the safeguarding of PII and detection of potential PII incidents.

DoD routinely employs safeguards, such as the following, to information systems and paper recordkeeping systems: Multifactor log-in authentication including common access card

authentication and password; system firewalls, physical token as required; physical and technological access controls governing access to data; network encryption to protect data transmitted over the network; disk encryption securing data at rest; key management services to safeguard encryption keys; masking of sensitive data as practicable; mandatory information assurance and privacy training for individuals who will have access; identification, marking, and safeguarding of PII; physical access safeguards including multifactor identification physical access controls, detection and electronic alert systems for access to servers and other network infrastructure; and electronic intrusion detection systems in DoD facilities.

RECORD ACCESS PROCEDURES: Individuals seeking access to their records should address written inquiries to the DoD OIG Freedom of Information Act (FOIA), Privacy and Civil Liberties Office, ATTN: Privacy Officer, 4800 Mark Center Drive, Alexandria, VA 22350-1500. Signed written requests should contain the name and number of this system of records notice along with the full name, mailing address and email address of the requester, along with any details which may assist in locating requested records, such as the case number and date of the event. In addition, the requester must provide either a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the appropriate format:

If executed outside the United States: “I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature).”

If executed within the United States, its territories, possessions, or commonwealths: “I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature).”

CONTESTING RECORD PROCEDURES: The DoD rules for accessing records, contesting contents, and appealing initial Component determinations are contained in 32 CFR part 310, or may be obtained from the system manager.

NOTIFICATION PROCEDURES: Individuals seeking to determine whether information about themselves is contained in this system of records should follow the instructions for Record Access Procedures above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: DoD has exempted records maintained in this system from 5 U.S.C. 552a(c)(3) and (4), (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8); (f); and (g) of the Privacy Act, pursuant to 5 U.S.C. 552a(j)(2). Additionally, DoD has exempted records maintained in this system from 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(1), (k)(2), and (k)(5). An exemption rule for this system has been promulgated in accordance with the requirements of 5 U.S.C. 553(b)(1), (2), and (3), and (c), and published in 32 CFR part 310.

In addition, when exempt records received from other systems of records become part of this system, DoD also claims the same exemptions for those records that are claimed for the original primary systems of records from which they originated and claims any additional exemptions set forth here.

HISTORY: March 17, 2016, 81 FR 14427; July 26, 2013, 78 FR 45185; October 15, 2008, 73 FR 61089; May 31, 2006, 71 FR 30882; May 9, 2003, 68 FR 24937; February 22, 1993, 58 FR 10213.

[FR Doc. 2022-11540 Filed: 5/27/2022 8:45 am; Publication Date: 5/31/2022]